# U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

## Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

**Name of Project:** DOI GovDelivery
**Bureau/Office:** Office of the Secretary (OS)
**Date:** September 17, 2021
**Point of Contact**
Name: Danna Mingo
Title: OS Departmental Offices Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: (202) 441- 5504
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

## Section 1. General System Information

### A. Is a full PIA required?

☒Yes, information is collected from or maintained on

- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No:

### B. What is the purpose of the system?

GovDelivery is a digital communications platform owned and operated by GovDelivery, Inc. located in Minnesota. GovDelivery is FedRamp authorized and is a Software as Service (SaaS) cloud service provider that provides a web-based application delivered via Government Community Cloud. GovDelivery is used exclusively by the government to elevate, streamline,

and track all the communication efforts with the public and to drive public engagements with the government programs and services. It enables the Department of the Interior (DOI) to provide a free email subscription and maximize its public outreach in a secured, trustful, and impactful manner.

The use of GovDelivery allows DOI to integrate graphics and multimedia content, deliver updates and newsletters to subscribers, and manage subscription preferences. Visitors to the DOI website have the option to enter their email addresses for GovDelivery to subscribe to the website's email notifications on topics they are interested in. GovDelivery allows DOI website visitors to subscribe quickly and easily based on their individual needs and interests.

The DOI Federal Consulting Group (FCG) contracted with GovDelivery manages the use of the GovDelivery digital communications service for the Department. DOI bureaus and offices use the GovDelivery service to facilitate communication and outreach for their respective program areas. Each bureau and office are responsible for ensuring use of GovDelivery is compliant with Federal laws, regulations, and policy.

**C. What is the legal authority?**

44 U.S.C. 3501, Paperwork Reduction Act of April 7, 2010; 5 U.S.C 301, Departmental Regulations; The President's January 21, 2009 memorandum on Transparency and Open Government; Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012; OMB Memorandum M-10-06, Open Government Directive, December 8, 2009; OMB Memorandum for the Heads of Executive Department Agencies, and Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies; and 110 Departmental Manual 5, Office of Communications.

**D. Why is this PIA being completed or modified?**

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

**E. Is this information system registered in CSAM?**

☒Yes:

System Security and Privacy Plan (SSP) for GovDelivery
UII Code: 010-000002301

☐ No

**F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.**

| Subsystem Name | Purpose | Contains PII *(Yes/No)* | Describe *If Yes, provide a description.* |
|---|---|---|---|
| None | None | No | N/A |

**G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?**

☒ Yes:

Some bureaus and offices may conduct outreach activities within their respective programs that operate under a published Privacy Act system of records notice for that specific bureau or office program. DOI has also published DOI-08, DOI Social Networks - 76 FR 44033 (July 22, 2011) system of record notice, which covers communications with individuals who contact DOI through social media outlets such as GovDelivery. DOI system of records notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

**H. Does this information system or electronic collection require an OMB Control Number?**

☐ Yes:
☒ No

## Section 2. Summary of System Data

**A. What PII will be collected? Indicate all that apply.**

☒Other:

The subscriber email address, which can be personal email address or official email address, specific websites individuals wish to receive notifications from, and subscription preferences. A subscriber may provide a password.

**B. What is the source for the PII collected? Indicate all that apply.**

☒Individual
☐ Federal agency
☐ Tribal agency

☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

**C. How will the information be collected? Indicate all that apply.**

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☒ Other: *Describe*

The DOI website at https://www.doi.gov directs the users to the GovDelivery website at https://public.govdelivery.com/accounts/USDOI/subscriber/topics where users can provide email addresses to subscribe to notifications via email on updates from DOI.

**D. What is the intended use of the PII collected?**

Email addresses are used to set up accounts and subscription preferences. They are used by DOI GovDelivery to deliver notifications about newly posted newsletters with topics in the subscriber's preference list.

**E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.**

☒Within the Bureau/Office:

Email addresses may be used internally within a bureau or office to manage user accounts and subscription preferences, and to deliver notifications about newly posted newsletters with topics in the subscriber's preference list.

☐ Other Bureaus/Offices:

☐ Other Federal Agencies:

☐ Tribal, State or Local Agencies:

☒Contractor:

GovDelivery receives the email addresses and subscription preferences directly from subscribers and will use the information to provide website content services.

☐ Other Third-Party Sources:

**F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?**

☒Yes:

Subscribing to the service is voluntary. Before users subscribe to the GovDelivery service, the user is presented with a DOI Privacy Notice for GovDelivery email updates, which details how the user's information will be handled by DOI and GovDelivery, and provides links to DOI and GovDelivery privacy policies. See https://www.doi.gov/privacy-GovDelivery.

Individuals may choose not to subscribe by clicking on the cancel button or not filling out the subscription form. Subscribers may also unsubscribe at any time by clicking "delete my account" button on the Subscription Preference page. When an individual unsubscribes, the email address is permanently deleted.

☐ No:

**G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

☐ Privacy Act Statement:

☒Privacy Notice:

A DOI Privacy Notice for GovDelivery email updates is provided when users subscribe to the service at https://public.govdelivery.com/accounts/USDOI/subscriber/topics, and details how the user's information will be handled by DOI and GovDelivery, and provides links to DOI and GovDelivery privacy policies. Please review the notice at https://www.doi.gov/privacy-GovDelivery.

Privacy Notice

The Department of the Interior (DOI) is pleased to offer a free e-mail subscription service to allow visitors to the DOI website to receive notifications by e-mail when new information is available. If you sign up for these automatic updates you will only receive notification of changes to the web pages you specify and may unsubscribe at any time. You will be asked to provide your email address and the updates you would like to receive. Providing this

information is voluntary; however, it is necessary in order to participate in this e-mail subscription service. This service is provided by a DOI contractor, GovDelivery, who will use the information you provide to deliver the notifications you have requested and to update your subscription preferences. DOI will have access to the information you provide to GovDelivery. DOI and GovDelivery will not share your personal information with third parties for promotional purposes. Please review the DOI Privacy Policy for how information is handled: http://www.doi.gov/privacy. You should also review the GovDelivery privacy policy to learn how GovDelivery uses your information. For additional guidance regarding how your information may be used, please see the DOI-08, DOI Social Networks, system of records notice (SORN) at 76 FR 44033 (July 22, 2011), or applicable DOI Bureau or office SORN for the program related to the subscription service. DOI SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy sorn.

☒Other:

Notice is also provided to users through the publication of this privacy impact assessment.

☐ None

**H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).**

Email addresses of subscribers are retrieved and used to send email notifications based on users' self-selected preferences.

**I. Will reports be produced on individuals?**

☐ Yes:
☒No

## Section 3. Attributes of System Data

**A. How will data collected from sources other than DOI records be verified for accuracy?**

Email addresses are collected from users who subscribe to the content services provided by DOI GovDelivery and are presumed to be accurate at the time the subscription is established. The users are responsible for the accuracy of the email addresses they provide and may unsubscribe or update their account preferences at any time.

**B. How will data be checked for completeness?**

Users are responsible for the completeness of the email addresses they provide when they subscribe to the service.

**C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).**

User email addresses are collected when users subscribe to the website content delivery service, and users are responsible for providing current email addresses. Users may unsubscribe or update their account preferences at any time. User accounts will be immediately deleted when the subscribers click "Delete my account". These procedures allow the contact information of the subscribers stay current.

**D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.**

Retention periods vary as records are maintained in accordance with the applicable records schedule specific to the program office utilizing GovDelivery to manage email subscriptions and disseminate email notifications. Records retention requirements must be assessed on a case by case basis depending on the bureau or office releasing the information, information released, the purpose of the release, and the needs of the agency.

DOI GovDelivery provides an email subscription service for information the government is releasing, so contents may be categorized as non-record (copies). The retention and disposition schedule of the user data that DOI GovDelivery maintains is authorized under Department Records Schedule -1, Administrative Records, 1.4-Information Technology (DAA-0048-2013-0001-0013), which was approved by the National Archives and Records Administration (NARA). The disposition is temporary, and records are cut off when superseded by a full backup of the system, and when no longer needed for system restoration.

**E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?**

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

**F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.**

There is a minimal impact to privacy as only a voluntarily provided email address is collected and used to establish email subscriptions. DOI GovDelivery is a digital communication platform used for driving the public engagement in DOI programs and services. DOI GovDelivery has implemented privacy and security controls to ensure that individual privacy is protected and privacy risks can be minimized so that the individuals can feel free to choose communication media and feel safe to engage in DOI's public outreach initiatives. Individuals self-select the email subscription and desired settings, and may also unsubscribe at any time by clicking the "delete my account" button on the Subscription Preference page. When an individual unsubscribes, the email address is permanently deleted.

DOI provides clear notice on the specific use and handling of email address information requested for subscriptions to the GovDelivery service. The GovDelivery website has self-deletion option for users to delete their account, and the immediate account deletion would become permanent. DOI only retains the system backup records which are superseded by a full backup of the system. The DOI Privacy Notice provided to subscribers also contains a link to the DOI Privacy Program website, which contains Privacy Act notices, privacy impact assessments, and privacy policies, standards, and procedures that may impact individual privacy. These notices, policies and standards promote transparency and provide notice to individuals on DOI's collection, use, maintenance and disposition of PII during interactions on DOI websites, social media applications, and with DOI programs.

GovDelivery is FedRAMP authorized and has undergone an independent third-party assessment. GovDelivery has undergone a formal Assessment and Authorization for issuance of an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and has been rated as a moderate system requiring strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system. GovDelivery provides email subscription services to Federal government agencies and follows National Institute of Standards and Technology (NIST) guidelines in implementing and managing its security policies and privacy controls. GovDelivery is responsible for preventing unauthorized access to the system and the data contained within the system.

The GovDelivery system infrastructure is hosted in a secure environment with five levels of physical security and access controls, and the data both in-transit and at rest are encrypted. DOI requires all its employees and service providers to take annual security, privacy awareness training, and role-based training to ensure the security and privacy awareness in accordance with Federal law and policy, and DOI information assurance and privacy policy.

## Section 4. PIA Risk Review

**A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

☒ Yes:

The email addresses of the subscribers are used to send notifications based on subscriber preferences.

☐ No

**B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?**

☐ Yes:

☒No

**C. Will the new data be placed in the individual's record?**

☐ Yes

☒No

**D. Can the system make determinations about individuals that would not be possible without the new data?**

☐ Yes:

☒No

**E. How will the new data be verified for relevance and accuracy?**

Not applicable as new data is not created.

**F. Are the data or the processes being consolidated?**

☐ Yes, data is being consolidated.
☐ Yes, processes are being consolidated.
☒ No, data or processes are not being consolidated.

**G. Who will have access to data in the system or electronic collection? Indicate all that apply.**

☒ Users
☒ Contractors
☐ Developers
☐ System Administrator
☒ Other: *Describe*

The subscribers can access, update, or delete their accounts. The GovDelivery contractors can access the email address to provide the service and for system maintenance. Each DOI bureau or office that uses GovDelivery can assign one administrator to maintain the program activity. DOI bureaus and offices are responsible for ensuring use of GovDelivery complies with Federal laws and policies.

**H. How is user access to data determined? Will users have access to all data or will access be restricted?**

Individual subscribers can only access their own account to manage their subscription preferences or delete their account.

System administrators (GovDelivery contractor) have access to the subscribers' email addresses to maintain the system function, and this access is based on need-to-know and least privilege principles.

**I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?**

☒ Yes. Privacy Act contract clauses and provisions are included in the contract to support the maintenance of the system

☐ No

**J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?**

☐ Yes.

☒No

**K. Will this system provide the capability to identify, locate and monitor individuals?**

☐ Yes.

☒No

**L. What kinds of information are collected as a function of the monitoring of individuals?**

Session cookies are used to allow subscribers to access and make changes to their profile. The session cookie stores the user's email address in order to identify the user and save changes. No persistent tracking is used on the subscription page or on User Profile pages.

**M. What controls will be used to prevent unauthorized monitoring?**

No persistent tracking is used on the subscription page or on User Profile pages. The transmission of user information is encrypted at the time subscriber information is provided. The stored subscriber information is also encrypted.

**N. How will the PII be secured?**

(1) Physical Controls. Indicate all that apply.

☒Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒Identification Badges
☐ Safes
☐ Combination Locks
☐ Locked Offices
☒Other. *Describe*

DOI GovDelivery also has access controls on output devices at the GovDelivery system site. GovDelivery is FedRAMP authorized and is subject to the NIST SP 800-53 security and privacy controls.

(2) Technical Controls. Indicate all that apply.

☒Password
☒Firewall
☒Encryption
☒User Identification
☐ Biometrics
☒Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒Personal Identity Verification (PIV) Card
☒Other. *Describe*

DOI GovDelivery operates in an environment with encrypted remote access control. GovDelivery is FedRAMP authorized and is subject to the NIST SP 800-53 security and privacy controls.

(3) Administrative Controls. Indicate all that apply.

☒Periodic Security Audits
☒Backups Secured Off-site
☒Rules of Behavior
☒Role-Based Training
☒Regular Monitoring of Users' Security Practices
☒Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Encryption of Backups Containing Sensitive Data
☒Mandatory Security, Privacy and Records Management Training

☒Other. *Describe*

GovDelivery is FedRAMP certified and is subject to the NIST SP 800-53 security and privacy controls.

**O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.**

FCG is the GovDelivery Information System Owner and is responsible for oversight and management of GovDelivery and ensuring adequate security and privacy controls are implemented. The GovDelivery Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the use and maintenance of GovDelivery. FCG and the bureau and office program officials using GovDelivery are responsible for addressing privacy issues or complaints for the specific uses within their area of responsibility in consultation with DOI privacy officials.

**P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?**

FCG is the GovDelivery Information System Owner and is responsible for oversight and management of the GovDelivery security and privacy controls, and for ensuring to the greatest possible extent that DOI data is properly managed and that all access to DOI data has been granted in a secure and auditable manner. Bureaus and offices are responsible for ensuring their use of GovDelivery is in accordance with Federal law and policy. The Information System Owner is responsible for ensuring that any potential or confirmed loss, compromise, unauthorized access or disclosure of PII is reported to the DOI Computer Incident Response Center (DOI-CIRC) within 1-hour of discovery in accordance with DOI policy and established procedures.